AMENDMENTS TO THE CLAIMS:

Pursuant to 37 C.F.R. § 1.121, the following listing of claims will replace all prior versions and listings of claims in the application.

Listing of the Claims:

1. (Currently amended) A method for preventing Ethernet from being attacked, comprising:

establishing and storing a fixed map between a port and a hardware address of a terminal device, ~~then forwarding a data packets according to the fixed map~~ after an Ethernet communication device detects a new connection between the port and the terminal device and receives ~~a the~~ data packet from the terminal device;

forwarding data packets according to the fixed map; ~~and~~

prohibiting the fixed map between the port and the hardware address from being modified as long as the connection between the port and the terminal device is not cut off; and

deleting the fixed map after the Ethernet communication device detects a disconnection between the port and the terminal device.

2. (Currently amended) The method of claim 1, further comprising: after receiving the data packet from the terminal device, judging whether the fixed map has been established; wherein:

if ~~so,~~ it is judged that the fixed map has been established, jumping to the step of forwarding the data packet; ~~otherwise,~~

if it is judged that the fixed map has not been established, jumping to the step of establishing and storing the fixed map between the port and the hardware address of the terminal device.

3. (Previously presented) The method of claim 2, wherein the forwarding of the data packets comprises judging whether a hardware address carried in the data packet is consistent with the hardware address corresponding to the port in said fixed map; if so, forwarding the data packet according to a conventional forwarding processing; otherwise, discarding the data packet.

4. (Previously presented) The method of claim 3, further comprising: after discarding the data packet, recording result of the judging of whether the address carried in the data packet is consistent with the hardware address corresponding to the port in said fixed map, in a log and informing a network administrator.

5. (Original) The method of claim 1, wherein said hardware address is a Media Access Control (MAC) address.

6. (Original) The method of claim 1, wherein detecting the new connection or the disconnection between the terminal device and the port is implemented by detecting physical signals in the port.

7. (Original) The method of claim 1, wherein said Ethernet communication device is a two-layer switch, a three-layer switch, a firewall device or an Ethernet bridge.

8. (Original) The method of claim 1, wherein said terminal device is a personal computer, a server or an IP telephone set.

9. (Original) The method of claim 1, wherein said fixed map is stored in a hardware address table of the Ethernet communication device.

10. (Currently amended) An Ethernet communication device for preventing Ethernet from being attacked, comprising:

means for establishing and storing a fixed map between a port and a hardware address of a terminal device after detecting a new connection between the port and the terminal device and receiving a data packet from the terminal device;

means for forwarding [a] data ~~packet~~ packets according to the fixed map ~~after detecting a new connection between the port and the terminal device and receiving the data packet from the terminal device~~;

means for prohibiting the fixed map between the port and the hardware address from being modified as long as the connection between the port and the terminal device is not cut off; and

means for deleting the fixed map after detecting a disconnection between the port and the terminal device.

11. (Previously presented) The Ethernet communication device of claim 10, further comprising:

means for judging whether a hardware address carried in the data packet is consistent with the hardware address corresponding to the port in said fixed map; if so, forwarding the data packet according to a conventional forwarding processing; otherwise, discarding the data packet.